Chapter 5
Evidence

A. Introduction

Although the primary concern of this manual is obtaining computer records in criminal investigations, prosecutors must also bear in mind the admissibility of that evidence in court proceedings. Computer evidence can present novel challenges. A complete guide to offering computer records into evidence is beyond the scope of this manual. However, this chapter addresses some of the more important evidentiary issues arising when the government seeks to admit computer records in court, including hearsay and the foundation to establish the authenticity of computer records.

B. Hearsay

Hearsay is "a *statement*, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Fed. R. Evid. 801(c) (emphasis added). "A 'statement' is (1) an oral or written *assertion* or (2) nonverbal conduct of a *person*, if it is intended by the *person* as an assertion." Fed. R. Evid. 801(a) (emphasis added). The Rules of Evidence do not define an "assertion." However, courts have held that "the term has the connotation of a positive declaration." *See, e.g.*, *United States v. Lewis*, 902 F.2d 1176, 1179 (5th Cir. 1990); *Lexington Ins. Co. v. W. Penn. Hosp.*, 423 F.3d 318, 330 (3d Cir. 2005).

Many courts have categorically determined that computer records are admissible under Federal Rule of Evidence 803(6), the hearsay exception for "records of regularly conducted activity"—or more commonly, the "business records" exception—without first asking whether the records are hearsay. *See, e.g., Haag v. United States,* 485 F.3d 1, 3 (1st Cir. 2007); *United States v. Fujii*, 301 F.3d 535, 539 (7th Cir. 2002); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990).

Increasingly, however, courts have recognized that many computer records result from a process and are not statements of persons—they are thus not

hearsay at all. *See United States v. Washington,* 498 F.3d 225, 230-31 (4th Cir. 2007) (printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay); *United States v. Hamilton,* 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated header information was not hearsay as "there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801"); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("nothing 'said' by a machine . . . is hearsay") (quoting 4 Mueller & Kirkpatrick, *Federal Evidence* § 380, at 65 (2d ed. 1994)).

This section addresses hearsay issues associated with three categories of computer records: (1) those that record assertions of persons (hearsay); (2) records resulting from a process (non-hearsay); and (3) records that combine the first two categories and thus are partially hearsay. This section also addresses Confrontation Clause issues that may arise when seeking admission of computer records. However, this section does not address in detail more general questions regarding the admission of hearsay, which are thoroughly addressed by other resources. *See, e.g., Courtroom Evidence, 2nd*, Article VIII, United States Department of Justice, OLE (2001); Steven Goode and Olin G. Welborn, *Courtroom Evidence Handbook*, Ch. 2, pp. 226-280 (2005-2006).

1. Hearsay vs. Non-Hearsay Computer Records

Records stored in computers can be divided into three categories: non-hearsay, hearsay, and records that include both hearsay and non-hearsay. First, non-hearsay records are created by a process that does not involve a human assertion, such as: telephone toll records; cell tower information; email header information; electronic banking records; Global Positioning System (GPS) data; and log-in records from an ISP or internet newsgroup. Although human input triggers some of theses processes—dialing a phone number or a punching in a PIN—this conduct is a command to a system, not an *assertion*, and thus is not hearsay. Second, hearsay records contain assertions by people, such as: a personal letter; a memo; bookkeeping records; and records of business transactions inputted by persons. Third, mixed hearsay and non-hearsay records are a combination of the first two categories, such as: email containing both content and header information; a file containing both written text and file creation, last written, and last access dates; chat room logs that identify the participants and note the time and date of "chat"; and spreadsheets with figures that have been typed in by a person, but the columns of which are automatically calculated by the computer program.

Non-Hearsay Records

Hearsay rules apply to statements made by persons, not to logs or records that result from computer processes. Computer-generated records that do not contain statements of persons therefore do not implicate the hearsay rules. This principle applies both to records generated by a computer without the involvement of a person (*e.g.*, GPS tracking records) and to computer records that are the result of human conduct other than assertions (*e.g.*, dialing a phone number or punching in a PIN at an ATM). For example, pressing "send" on an email is a command to a system (send this message to the person with this email address) and is thus non-assertive conduct. *See United States v. Bellomo*, 176 F.3d 580, 586 (2d Cir. 1999) ("Statements offered as evidence of commands or threats or rules . . . are not hearsay.").

Two cases illustrate this point. In *United States v. Washington*, 498 F.3d 225 (4th Cir. 2007), lab technicians ran a blood sample taken from the defendant through a gas chromatograph connected to a computer. The test results, signed by the lab director, indicated that the defendant had been driving under the influence of both alcohol and PCP. The lab director, who did not participate in testing the sample, testified at trial. The Fourth Circuit rejected a hearsay objection to this evidence. The court noted that the computer-generated test result was "data generated by" a machine and observed that hearsay must be a "statement" made by a "declarant." *Id.* at 231. Further, "[o]nly a *person* may be a declarant and make a statement." *Id.* Since "nothing 'said' by a machine . . . is hearsay," the Fourth Circuit concluded that the test results were not excludable based upon the hearsay rules. *Id.* (citation omitted).

Similarly, in *United States v. Hamilton,* 413 F.3d 1138 (10th Cir. 2005), the defendant made a hearsay objection to the admission of header information associated with approximately forty-four images introduced in his child pornography trial. The header information circumstantially identified Hamilton as the person who had posted the child pornography images to a "newsgroup." Specifically, the header information consisted of the subject of the posting, the date the images were posted, and Hamilton's screen name and IP address. *See id.* at 1142. The Tenth Circuit noted that the header information was "automatically generated by the computer hosting the newsgroup" when images were uploaded to the newsgroup. *Id.* Since the information was independently generated by the computer process, there was no "statement" by a "declarant" and thus the header information was "outside of Rule 801(c)'s definition of 'hearsay.'" *Id.* (citing *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.

2003) (header information automatically generated by a fax machine was not hearsay as "nothing 'said' by a machine . . . is hearsay.")).

Occasionally, courts have mistakenly assumed that computer-generated records are hearsay without recognizing that they do not contain the statement of a person. For example, in *United States v. Blackburn*, 992 F.2d 666 (7th Cir. 1993), a bank robber left his eyeglasses behind in an abandoned stolen car. The prosecution's evidence against the defendant included a computer printout from a machine that tests the curvature of eyeglass lenses; the printout revealed that the prescription of the eyeglasses found in the stolen car exactly matched the defendant's. At trial, the district court assumed that the computer printout was hearsay, but it concluded that the printout was an admissible business record according to Rule 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout was hearsay, but agreed with the defendant that the printout should not have been admitted as a business record. *See id.* at 670. Nevertheless, the court held that the computer printout was sufficiently reliable that it could have been admitted under Rule 807, the residual hearsay exception. *See id.* at 672. However, the court should instead have asked whether the computer printout from the lens-testing machine contained hearsay at all. This question would have revealed that the computer-generated printout could not be excluded properly on hearsay grounds (or on Confrontation Clause grounds—*see* Section B.2 *infra*) because it contained no human "statements."

Hearsay Records

Some computer records are wholly hearsay (*e.g.*, a printed text document describing observations of fact where the underlying file data is not introduced). Other computer records contain both hearsay and non-hearsay components (*e.g.*, an email with both header information and content that includes factual assertions). In each instance, the proponent must lay a foundation that establishes both the admissibility of the hearsay statement and the authenticity of the computer-generated record.

A number of courts permit computer-stored business records to be admitted as records of a regularly conducted activity under Rule 803(6). Where business records include hearsay, one must show through testing or by a certification complying with Rule 902(11) or 18 US.C. § 3505 that the records were contemporaneously made and kept in the normal and ordinary course of business by a person with knowledge. Different circuits have

articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Rule 803(6). *See, e.g.*, *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988). Other circuits have articulated doctrinal tests specifically for computer records that largely (but not exactly) track the requirements of Rule 803(6). *See, e.g.*, *United States v. Cestnik,* 36 F.3d 904, 909-10 (10th Cir. 1994) ("Computer business records are admissible if (1) they are kept pursuant to a routine procedure designed to assure their accuracy, (2) they are created for motives that tend to assure accuracy (*e.g.*, not including those prepared for litigation), and (3) they are not themselves mere accumulations of hearsay.") (internal quotation marks and citation omitted); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990) (computer-stored records are admissible business records if they "are kept in the course of regularly conducted business activity, and [it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness."). Notably, the printout itself may be produced in anticipation of litigation without running afoul of the business records exception. The requirement that the record be kept "in the course of a regularly conducted business activity" refers to the underlying data, not the actual printout of that data. *See United States v. Fujii*, 301 F.3d 535, 539 (7th Cir. 2002); *United States v. Sanders*, 749 F.2d 195, 198 (5th Cir. 1984).

In addition to the business records exception, other hearsay exceptions may apply in appropriate cases, such as the public records exception of Rule 803(8). *See, e.g.*, *United States v. Smith,* 973 F.2d 603, 605 (8th Cir. 1992) (police computer printouts are admissible as evidence); *Hughes v. United States*, 953 F.2d 531, 540 (9th Cir. 1992) (computerized IRS printouts are admissible). Computer records, particularly emails or chat logs, may also include admissions or adopted admissions, which are not hearsay under Rule 801(d)(2). For example, in *United States v. Burt*, 495 F.3d 733, 738-39 (7th Cir. 2007), the court found that logs of chat conversations between the defendant and a witness were not hearsay—the defendant's half of the conversation constituted "admissions" while the witness's half was admissible as context for those admissions. Similarly, in *United States v. Safavian*, 435 F. Supp. 2d 36, 43-44 (D.D.C. 2006), the full text of some emails forwarded by the defendant to others were admitted as "adoptive admissions" when their context clearly manifested the defendant's belief in the truth of the authors' statements.

2. Confrontation Clause

In *Crawford v. Washington*, 541 U.S. 36, 68 (2004), the Supreme Court held that the Confrontation Clause of the Sixth Amendment bars the government from introducing pre-trial "testimonial statements" of an unavailable witness unless the defendant had a prior opportunity to cross examine the declarant. *Id.* at 68. The *Crawford* Court declined to define "testimonial statements," but the courts of appeals have subsequently interpreted "testimonial" to mean those statements where the "declarant reasonably expected the statement to be used prosecutorially." *United States v. Ellis,* 460 F.3d 920, 925 (7th Cir. 2006) (collecting cases).

In *Melendez-Diaz v. Massachusetts*, 129 S.Ct. 2527, 2532 (2009), the Supreme Court recently held that "certificates of analysis" —affidavits from the state's forensic examiners—identifying substances found on a defendant as cocaine were testimonial statements under *Crawford*. At trial, the prosecution introduced the certificates to prove that the substance found on the defendant was in fact cocaine, and the affidavits themselves "contained only the bare-bones statement that '[t]he substance was found to contain: Cocaine.'" *Id.* at 2532. There was no dispute that the "certificates" at issue represented statements of persons. Rather, the respondents had argued, *inter alia*, that testimony concerning "neutral scientific testing" was more reliable and trustworthy than testimony concerning historical events and thus was not the type of testimonial statement that fell within the ambit of the Confrontation Clause. *See id.* at 2536-37. The Court rejected this distinction in favor of uniform treatment of all testimonial statements for Confrontation Clause purposes. *See id.* at 2532.

Although Confrontation Clause analysis is distinct from hearsay analysis, records that are the output of a computer-generated process do not implicate the Confrontation Clause for the same reason that computer-generated records are not hearsay: they are not statements of persons. In *United States v. Washington,* 498 F.3d 225 (4th Cir. 2007), as described above, computer-generated lab results indicated that the defendant had been driving under the influence of both alcohol and PCP. Washington argued that the computer-generated lab results were "testimonial hearsay" and thus violated his right to confront witnesses against him—namely, the lab technicians who actually ran the lab test. The Fourth Circuit rejected the Confrontation Clause argument, holding that the computer-generated test results were not statements "made by the technicians who tested the blood." *Id.* at 229. Rather, the "machine printout is the only source of the statement, and no *person* viewed a blood sample and concluded

that it contained PCP and alcohol." *Id.* The Sixth Amendment guarantees the right to confront witnesses; machines, not being persons, are not witnesses. Since the technicians, independent from the machine, could not have affirmed or denied the test results, the admission of the gas chromatography printout did not implicate the defendant's Sixth Amendment rights. In sum, the Fourth Circuit held that the "raw data generated by the diagnostic machines are 'statements' *of the machines* themselves, not their operators. But 'statements' made by machines are not out-of-court statements made by declarants that are subject to the Confrontation Clause." *Id.*

The Fourth Circuit's analysis in *Washington* is distinguishable from *Melendez-Diaz*. The document at issue in *Washington* was raw, computer-generated data, whereas the "certificates" at issue in *Melendez-Diaz* were plainly witness statements. Moreover, in *Washington*, the forensic scientist who interpreted the raw data testified as an expert, and thus the defendant had a full and fair opportunity to call into question the judgment and skills upon which his interpretation of any underlying data was based. *See Washington*, 498 F.3d at 228. The Fourth Circuit in *Washington* did not rely on the reliability of "neutral" scientific testing, but on the fact that the machine generating the data was not a person. Consequently, the Fourth Circuit's reasoning in *Washington* likely remains good law.

C. Authentication

Before a party moves for admission of an electronic record or any other evidence, the proponent must show that it is authentic. That is, the proponent must offer evidence "sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). *See United States v. Salcido,* 506 F.3d 729, 733 (9th Cir. 2007) (data from defendant's computer was properly introduced under Rule 901(a) based on "chain of custody"); *United States v. Meienberg*, 263 F.3d 1177, 1181 (10th Cir. 2001) (district court correctly found that sufficient evidence existed under Rule 901(a) to admit computer printout of firearms sold through defendant's business). The proponent need not prove beyond all doubt that the evidence is authentic and has not been altered. *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007). Instead, authentication requirements are "threshold preliminary standard[s] to test the reliability of the evidence, subject to later review by an opponent's cross-examination." *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 544 (D. Md. 2007) (citing Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.06 [3]

(Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997)); *see also United States v. Tin Yat Chin*, 371 F.3d 31, 37-38 (2d Cir. 2004). Once evidence has met this low admissibility threshold, it is up to the fact finder to evaluate what weight to give the evidence. *United States v. Ladd*, 885 F.2d 954, 956 (1st Cir. 1989).

1. Authentication of Computer-Stored Records

The standard for authenticating computer records is the same as for authenticating other records. Although some litigants have argued for more stringent authenticity standards for electronic evidence, courts have resisted those arguments. *See, e.g., United States v. Simpson*, 152 F.3d 1241, 1249-50 (10th Cir. 1998) (applying general rule 901(a) standard to transcript of chat room discussions); *In re F.P.*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005) ("We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.").

Generally, witnesses who testify to the authenticity of computer records need not have special qualifications. In most cases, the witness does not need to have programmed the computer himself or even understand the maintenance and technical operation of the computer. *See United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001) ("[I]t is not necessary that the computer programmer testify in order to authenticate computer-generated records."); *United States v. Moore*, 923 F.2d 910, 914-15 (1st Cir. 1991) (holding that head of bank's consumer loan department could authenticate computerized loan data). Instead, the witness simply must have first-hand knowledge of the relevant facts, such as what the data is and how it was obtained from the computer or whether and how the witness's business relies upon the data. *See generally United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (holding that FBI agent who was present when the defendant's computer was seized appropriately authenticated seized files).

Federal Rule of Evidence 901(b) offers a non-exhaustive list of authentication methods. Several of these illustrations are useful in cases involving computer records. For example, Rule 901(b)(1) provides that evidence may be authenticated by a person with knowledge "that a matter is what it is claimed to be." *See United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (witness and undercover agent sufficiently authenticated emails and chat log

exhibits by testifying that the exhibits were accurate records of communications they had had with the defendant); *United States v. Kassimu*, 2006 WL 1880335 (5th Cir. Jul. 7, 2006) (district court correctly found that computer records were authenticated based on the Postal Inspector's description of the procedure employed to generate the records).

Rule 901(b)(3) allows authentication of the item where the trier of fact or an expert compares it "with specimens which have been authenticated." *See United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails that were not clearly identifiable on their own could be authenticated by comparison to other emails that had been independently authenticated). Rule 901(b)(4) indicates that evidence can be authenticated based upon distinctive characteristics such as "contents, substance, internal patterns, or other distinctive characteristics." *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email was appropriately authenticated based entirely on circumstantial evidence, including presence of the defendant's work email address, information within the email with which the defendant was familiar, and use of the defendant's nickname); *Safavian*, 435 F. Supp. 2d at 40 (distinctive characteristics for email included the "@" symbol, email addresses containing the name of the person connected with the email, and the name of the sender or recipient in the "To," "From," or signature block areas).

Rule 901(b)(4) is helpful to prosecutors who seek to introduce electronic records obtained from seized storage media. For example, a prosecutor introducing a hard drive seized from a defendant's home and data from that hard drive may employ a two-step process. First, the prosecutor may introduce the hard drive based on chain of custody testimony or its unique characteristics (*e.g.*, the hard drive serial number). Second, prosecutors may consider using the "hash value" or similar forensic identifier assigned to the data on the drive to authenticate a copy of that data as a forensically sound copy of the previously admitted hard drive. Similarly, prosecutors may authenticate a computer record using its "metadata" (information "describing the history, tracking, or management of the electronic document"). *See Lorraine v. Markel American Ins. Co.,* 241 F.R.D. at 547-48.

When computer-stored records are records of regularly conducted business activity, Rule 902(11) (domestic records) and 18 U.S.C. § 3505 (foreign records) permit the use of a written certification to establish the authenticity of the record. Some have questioned whether such certifications constitute testimonial hearsay barred by *Crawford v. Washington*, 541 U.S. 36 (2004),

which is discussed in Section B.2 above. *See, e.g., United States v. Jimenez*, 513 F.3d 62, 78 (3d Cir. 2008) ("Even assuming, without deciding, that the Rule 902(11) declarations are testimonial and subject to the Confrontation Clause, their admission in this case for the purpose of authenticating the bank statements was harmless."). In dicta in *Melendez-Diaz*, the Supreme Court noted that under common law, "[a] clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record." *Melendez-Diaz v. Massachusetts*, 129 S. Ct. 2527, 2539 (2009). Lower courts may follow this statement from *Melendez-Diaz* and hold that the Confrontation Clause allows the introduction of certificates of authenticity at trial. Moreover, even if the Confrontation Clause did bar the introduction of certificates of authenticity at trial, the certificates likely could still be used to establish the authenticity of the records under Rule 104(a), which specifies that "[p]reliminary questions concerning . . . the admissibility of evidence shall be determined by the court," and that in making admissibility determinations, the court "is not bound by the rules of evidence except those with respect to privileges." *See United States v. Collins*, 966 F.2d 1214, 1223 (7th Cir. 1992) ("In *Bourjaily v. United States*, 483 U.S. 171, 175-76 (1987), the Supreme Court held that a judge can, without offending the Sixth Amendment's Confrontation Clause, consider another person's out-of-court statements in determining whether these statements are admissible as coconspirator statements.").

2. Authentication of Records Created by a Computer Process

Records that are not just stored in a computer but rather result, in whole or part, from a computer process will often require a more developed foundation. To demonstrate authenticity for computer-generated records, or any records generated by a process, the proponent should introduce "[e]vidence describing a process or a system used to produce a result and showing that the process or system produces an accurate result." Fed. R. Evid. 901(b)(9). *See also United States v. Briscoe*, 896 F.2d 1476, 1494-95 (7th Cir. 1990) (the government satisfied its burden where it provided sufficient facts to warrant a finding that the records were trustworthy and the opposing party was afforded an opportunity to inquire into the accuracy thereof). Moreover, in addition to the obvious benefit of getting the records into evidence, a developed foundation will explain what the computer or program does, thereby enabling the finder of fact to understand the soundness and relevance of the records.

In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such

as in the ordinary course of business.[1] *See, e.g., United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001) ("evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business" was sufficient for establishing trustworthiness); *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, . . . at least where absolutely nothing in the record in any way implies the lack thereof."). While expert testimony may be helpful in demonstrating the reliability of a technology or computer process, such testimony is often unnecessary. *See Salgado*, 250 F.3d at 453 ("The government is not required to present expert testimony as to the mechanical accuracy of the computer where it presented evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business."); *Brown v. Texas*, 163 S.W.3d 818, 824 (Tex. App. 2005) (holding that witness who used global positioning system technology daily could testify about technology's reliability).

When the computer program is not used on a regular basis and the proponent cannot establish reliability based on its use in the ordinary course of business, the proponent may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970). Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988); *see also United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000).

[1] As discussed in the hearsay section of this chapter, federal courts that evaluate the authenticity of computer-generated records sometimes assume that the records contain hearsay and then apply the business records exception. *See, e.g., Salgado*, 250 F.3d at 452-53 (applying business records exception to telephone records generated "automatically" by a computer); *United States v. Linn*, 880 F.2d 209, 216 (9th Cir. 1989) (same). Although this analysis is technically incorrect when the records do not contain statements of a person, as a practical matter, prosecutors who lay a foundation to establish a computer-generated record as a business record will also lay the foundation to establish the record's authenticity. Evidence that a computer program is sufficiently trustworthy so that its results qualify as business records under Fed. R. Evid. 803(6) also establishes the authenticity of the record. *Cf. United States v. Saputski,* 496 F.2d 140, 142 (9th Cir. 1974).

3. Common Challenges to Authenticity

Alterations

Because electronic records can be altered easily, opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. Importantly, courts have rejected arguments that electronic evidence is inherently unreliable because of its potential for manipulation. As with paper documents, the mere possibility of alteration is not sufficient to exclude electronic evidence. Absent specific evidence of alteration, such possibilities go only to the evidence's weight, not admissibility. *See United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D.D.C. 2006). *See also United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997); *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible.").

Nevertheless, prosecutors and investigators should be wary of situations in which evidence has been edited or is captured using methods subject to human error. In *United States v. Jackson*, 488 F. Supp. 2d 866 (D. Neb. 2007), an undercover agent had recorded chat sessions with the defendant by "cutting and pasting" the log of each conversation into a word processing document. After his investigation ended, the agent's computer was wiped clean, leaving the "cut and paste" document as the only record of the chat conversations. Despite the agent's testimony at trial that he had been careful to avoid errors in cutting and pasting, the court excluded the "cut and paste" document based on defense expert testimony that suggested errors in the agent's transcript. *Id.* at 869-71. The court's analysis relied, in part, on the defense expert's testimony that there were several more reliable methods that the agent could have used to accurately capture the chat logs, including creating a forensic image of the agent's computer's hard drive, using software to save the chats, or using a basic "print screen" function. *Id.* Still, the ruling in *Jackson* is at odds with the prevailing standard for authenticity, particularly given the agent's testimony that no errors were made and the defense's inability to demonstrate any actual, as opposed to hypothetical, errors. Under the prevailing standard, courts should admit even

"cut and paste" documents in many contexts. *Cf. United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (transcript of instant message conversations that were cut and pasted into word processing documents were sufficiently authenticated by testimony of a participant in the conversation).

Authorship

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records do not necessarily identify their author. This is a particular problem with Internet communications, which can offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous emails, and Internet Relay Chat channels permit users to communicate without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

Circumstantial evidence generally provides the key to establishing the authorship of a computer record. In particular, distinctive characteristics like email addresses, nicknames, signature blocks, and message contents can prove authorship, at least sufficiently to meet the threshold for authenticity. For example, in *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron" and sought to show that "Stavron" was the defendant. On appeal following his conviction, Simpson argued that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. *Id*. at 1249.

The Tenth Circuit rejected this argument, noting the considerable circumstantial evidence that "Stavron" was the defendant. *See id.* at 1250. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. *See id*.

at 1250; *see also United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails between defendant government official and lobbyist were authenticated by distinctive characteristics under Rule 901(b)(4) including email addresses which bore the sender's and recipient's names; "the name of the sender or recipient in the bodies of the email, in the signature blocks at the end of the email, in the 'To:' and 'From:' headings, and by signature of the sender"; and the contents); *United States v. Tank*, 200 F.3d 627, 630-31 (9th Cir. 2000) (district court properly admitted chat room log printouts in circumstances similar to those in *Simpson*); *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email messages were properly authenticated where messages included defendant's email address, defendant's nickname, and where defendant followed up messages with phone calls).

Authenticating Contents and Appearance of Websites

Several cases have considered what foundation is necessary to authenticate the contents and appearance of a website at a particular time. Print-outs of web pages, even those bearing the URL and date stamp, are not self-authenticating. *See In re Homestore.com, Inc. Securities Lit.*, 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004). Thus, courts typically require the testimony of a person with knowledge of the website's appearance to authenticate images of that website. *See id*. ("To be authenticated, some statement or affidavit from someone with knowledge is required; for example, Homestore's web master or someone else with personal knowledge would be sufficient."); *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir. 2007) (court cannot assume that a website belonged to a particular business based solely on the site's URL); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (web postings purporting to be statements made by white supremacist groups were properly excluded on authentication grounds absent evidence that the postings were actually posted by the groups). Testimony of an agent who viewed a website at a particular date and time should be sufficient to authenticate a print-out of that website.

Some litigants have attempted to introduce content from web pages stored by the Internet Archive, a non-profit organization attempting to create a "library" of web pages by using automated web crawlers to periodically capture web page contents. Internet Archive provides a service called the "Wayback Machine" that enables users to view historical versions of captured web pages on a given date. The various courts that have considered information obtained through the Wayback Machine have differed over whether testimony about the Internet Archive's operation is sufficient or whether proponents must provide

testimony from someone with personal knowledge of the particular web pages' contents. *Compare St. Luke's Cataract and Laser Institute v. Sanderson*, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006) (Internet Archive employee with personal knowledge of the Archive's database could authenticate web pages retrieved from the Archive), *and Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (affidavit from an Internet Archive employee would be sufficient to authenticate web pages retrieved from the Internet Archive's database if the employee had personal knowledge of the Archive's contents), *with Novak v. Tucows, Inc.*, 2007 WL 922306, at *5 (E.D.N.Y. Mar. 26, 2007) (requiring testimony from the host of a web page, rather than from the Internet Archive, to authenticate the page's contents).

D. Other Issues

The authentication requirement and the hearsay rule usually constitute the most significant hurdles that prosecutors will encounter when seeking the admission of computer records. However, some agents and prosecutors have occasionally considered two additional issues: the application of the best evidence rule to computer records and whether computer printouts are "summaries" that must comply with Fed. R. Evid. 1006.

1. The Best Evidence Rule

The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required. *See* Fed. R. Evid. 1002. For example, in *United States v. Bennett*, 363 F.3d 947, 953 (9th Cir. 2004), in an effort to prove that the defendant had imported drugs from international waters, an agent testified about information he viewed on the screen of the global positioning system (GPS) on the defendant's boat. The Ninth Circuit found that the agent's testimony violated the best evidence rule. The agent had only observed a graphical representation of data recorded by the GPS system; he had not actually observed the boat following the purported path. Because the United States sought to prove the contents of the GPS data, the best evidence rule required the government to introduce the GPS data itself or the printout of that data, rather than merely the agent's testimony about the data. *See id.* Alternatively, the government could have sought to demonstrate that the original GPS data was lost, destroyed, or

otherwise unobtainable under Fed. R. Evid. 1004, but the court ruled that the government had failed to do. *See id*. at 954.

Agents and prosecutors occasionally express concern that a mere printout of a computer-stored electronic file may not be an "original" for the purpose of the best evidence rule. After all, the original file is merely a collection of 0's and 1's; in contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes.

The Federal Rules of Evidence have expressly addressed this concern. The Rules state that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'." Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. *See Doe v. United States*, 805 F. Supp. 1513, 1517 (D. Haw. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality:

> While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout.

Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972).

However, as with demonstrating authenticity, a proponent might need to demonstrate that the print out does *accurately* reflect the stored data in order to satisfy the best evidence rule. *Compare Laughner v. State*, 769 N.E. 2d 1147, 1159 (Ind. Ct. App. 2002) (AOL Instant Message logs that police had cut-and-pasted into a word-processing file satisfied best evidence rule) (*abrogated on other grounds by Fajardo v. State*, 859 N.E. 2d 1201 (Ind. 2007)), *with United States v. Jackson,* 488 F. Supp. 2d 866, 871 (D. Neb. 2007) (word-processing document into which chat logs were cut-and-pasted was not the "best evidence" because it did not accurately reflect the entire conversation).

Similarly, properly copied electronic data is just as admissible as the original data. Rule 1003 states that a "duplicate is admissible to the same extent as an original" unless there is a genuine question about the original's authenticity or there is some other reason why admitting the duplicate would be unfair. A "duplicate" is defined, by Rule 1001(4), as "a counterpart produced by the same

impression as the original . . . or by mechanical or electronic re-recording . . . or by other equivalent techniques which accurately reproduces the original." Thus, a proponent can introduce, for instance, an image of a seized hard drive, where the proponent can demonstrate that the imaging process accurately copied the data on the original hard drive. This demonstration is often accomplished through testimony showing that the hash value of the copy matches that of the original.

2. Computer Printouts as "Summaries"

Federal Rule of Evidence 1006 permits parties to offer summaries of voluminous evidence in the form of "a chart, summary, or calculation" subject to certain restrictions. Agents and prosecutors occasionally ask whether a computer printout is necessarily a "summary" of evidence that must comply with Fed. R. Evid. 1006. In general, the answer is no. *See United States v. Moon*, 513 F.3d 527, 544-45 (6th Cir. 2008); *United States v. Catabran*, 836 F.2d 453, 456-57 (9th Cir. 1988); *United States v. Sanders*, 749 F.2d 195, 199 (5th Cir. 1984); *United States v. Russo*, 480 F.2d 1228, 1240-41 (6th Cir. 1973). Of course, if the computer printout is merely a summary of other admissible evidence, Rule 1006 will apply just as it does to other summaries of evidence. *See United States v. Allen*, 234 F.3d 1278, 2000 WL 1160830, at *1 (9th Cir. Aug. 11, 2000).